increases, it is both necessary and important to ensure that government surveillance authority is clearly defined and appropriately limited. Id. at 16. The Joint Petition does not attempt to define the authority it argues should be given to law enforcement; instead it uses broad generalizations and extreme hypotheticals to force industry to comply with their needs, regardless of constitutionality, when developing technology.

In order to protect non-targeted communications and privacy in general, the FCC should not incorporate the Joint Petition-suggested standards for pen registers, location tracking, and call-identifying information. Instead, it should look to the language of the statute, the explicit statements of the House Committee Reports, and the statements by Director Freeh, on which Congress heavily relied in order to pass this legislation.

The call-identifying information requirements proposed in the Joint Petition far exceed the language and legislative intent of CALEA. In general, the Joint Petition advocates a "broad definition" of call-identifying information, claiming that "Congress demonstrated an intent to provide law enforcement with meaningful information that would enable it to understand the status of the call." Jt. Pet. ¶59. Congress did no such thing: In fact, Congress explicitly stated that law enforcement and the FCC should narrowly interpret CALEA, and further, that CALEA should not in any way expand law enforcement's wiretapping reach.

Specifically, the Joint Petition argues that, in addition to the call-identifying information associated with the initiation and completion of a call

detailed in the industry interim standard, law enforcement needs 1) access to subject-initiated dialing and signaling activity; 2) messages indicating whether a party is connected to a multi-party call at any given time; and 3) notification messages for network-generated in-band and out-of-band signaling. Jt. Pet. ¶60-64. None of these services were included or contemplated by the Congress. "The term 'call-identifying information' means the dialing or signaling information generated that identifies the origin and destination of a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization. . . Other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information." H.Rep. 103-827 at 21 (emphasis added). Even Director Freeh agreed that "[call-identifying information] relates to dialing type information. Senate Hearing at 33 (March 18, 1994 Statement). Both subject-initiated dialing activity and in-band and out-of-band signaling are explicitly dial tones generated by the sender to the recipient, and do not impact either the origin or the destination of communications; therefore they are beyond the scope of law enforcement's access to information.

The need to know whether the target is on a conference call is a new request, one that is inconsistently argued in the Joint Petition. Law enforcement agreed with statutes, Congressional intent, and case law that it must minimize the interference with non-targeted communications. 18 U.S.C. § 2518(5); 47 U.S.C. §1006(b)(2). See e.g., H.Rep. 103-827 at 16, 22; Jt. Pet. ¶8; Statement of Louis

Freeh, House Energy Committee, Subcommittee on Telecommunications and Finance, September 13, 1994 Hearing. They then posit that, despite all legal authority to the contrary and in absence of any stated interest during the legislative process, law enforcement must have complete access to all conference calls, regardless of whether the targeted subject continues to listen or be on the line. Jt. Pet. ¶¶51-55. This clearly does not minimize interference with non-targeted communications. The Joint Petition then states that it should know who is participating in conference calls (party drop, party hold, party join information). Jt. Pet. ¶60. If the intent of law enforcement was to restrict access to only those communications by the target, access to this information would make sense. However, if law enforcement wants to simultaneously listen to the entire conference call while at the same time learning when and what parties have been added, that sweeping access to communications would be an unconstitutional intrusion into the privacy of the non-targeted parties.

The information requested in the Joint Petition's discussion of pen registers specifically is similarly as expansive as the discussion of call-identifying information generally. Using pen registers as an analogy, the Joint Petition attempts to bootstrap the tonal information acquired, such as call waiting and hold, to allow that access for all wiretaps. Jt. Pet. ¶¶58-59. However, both Freeh and Congress requested that, whenever possible, pen register technology be restricted to "the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing," (September 13, 1994 Energy Com.

Hrg, Freeh) and to minimize the information the information obtained through pen registers. H.Rep.103-827 at 17. This intent is incompatible with the Joint Petition's bootstrapping attempt.

Further, the Joint Petition's disingenuous statements about industry's desire to comply with law enforcement needs cast doubt on the FBI's willingness to cooperate with industry officials. After eight years of discussions, repeated congressional hearings and proposed standards from both parties, the Joint Petition dismisses the industry good will and intentions by claiming that "several industry executives made clear that these needs would be met only if there were legislation so requiring." Jt. Pet. ¶22. What industry executives said candidly, and what Director Freeh testified (the source of the Joint Petition statement) was that, given market economics, mandatory legislation would be a way of incorporating both sides' concerns without individual companies unilaterally investing time, money and technical resources to develop solutions if there was no assurance that their competitors would do so. Senate Hearings at 26 (March 13, 1994 Statement, Freeh). Instead of allowing industry and law enforcement to work together, as Freeh promised in 1994, the Joint Petition wants to force technological solutions and expanded surveillance techniques onto the telecommunications industry, and onto the American public.

The Joint Petition also proposes that law enforcement gain access to location information of the target, against every statement of intent by lawmakers and Director Freeh. Director Freeh emphatically stated that the FBI so supported

the restriction of location information from law enforcement that "we are prepared to add a concluding phrase to this definition to explicitly clarify the point: . . . 'except that such [call-identifying] information shall not include any information that may disclose the physical location of a mobile facility or service beyond that associated with the number's area code or exchange'." Senate Hearings at 33 (March 18, 1994 Statement of Freeh). The Committee Report mirrored Freeh's strong language, repeatedly stating that no tracking or location information, other than that which can be determined from the phone number, may be included in pen registers or trap and traces. See H.Rep. 103-827 at 17, 22.

The Joint Petition only briefly asks for location information to be included in the definition of "call-identifying information," using a fanciful and far-fetched hypothetical of a call for an immediate "contract murder" where law enforcement is tapping the line, but they are unable to stop the murder because they cannot promptly discover whom has been called, or where the hit man is located. Jt. Pet. ¶ 87. In such a situation, the hit man's exact location should not be a concern, the intended victim's should be, and in the extreme hypothetical raised by the FBI, the victim's location will continue to be a mystery, regardless of location information of the caller and hit man.

The word "location" is never mentioned in that passage, in part to avoid the appearance of inconsistency within the FBI, but also to avoid the scorn and attention of the Members of Congress who believed Director Freeh when he said that law enforcement was not interested in obtaining exact locations for

targeted communications. However, regardless of semantics and shell games, no hypotheticals will change the law: no location information, other than that provided by area code and phone number, can be revealed through call-identifying information.

IV. Conclusion

As Congress and FBI Director Louis Freeh made clear, CALEA was enacted specifically to preserve, in the context of new technologies, the status quo in the government's electronic surveillance capabilities.48/ It "was intended to provide law enforcement no more and no less access to information" than law enforcement had had prior to CALEA's enactment.49/ In enacting CALEA, Congress struck a careful balance between, on one hand, "preserv[ing] a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts,"50/ and, on the other hand, "protect[ing] privacy in the face of increasingly powerful and personally revealing technologies."51/ The statute should be interpreted and implemented in accordance with the express intent of Congress. Indeed, the House Report on CALEA states that Congress "expects industry, law enforcement and the [Federal Communications Commission] to narrowly interpret the [carrier

---

48/ House Report at 3502.

49/ Id.

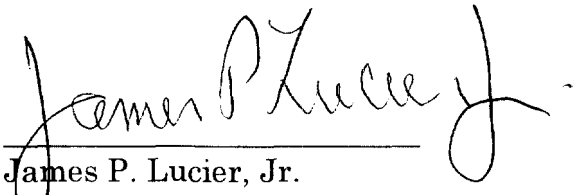
50/ Id. at 3493.

51/ Id.

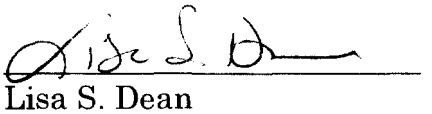
assistance] requirements" set forth in Section 103.52/ Any attempt to do otherwise will violate not only the letter and spirit of CALEA, but also the vital privacy protections established by the Fourth Amendment to the United States Constitution.

For the foregoing reasons, we respectfully request that the Commission reject the Joint Petition submitted by the FBI and DOJ.

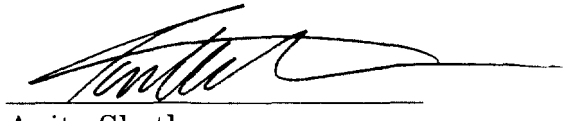
Respectfully submitted,



James P. Lucier, Jr.
Director of Economic Research
Americans for Tax Reform
1320 18th Street, NW, Suite 200
Washington, D.C. 20036



Lisa S. Dean
Director, Center for Technology Policy
Free Congress Foundation
717 Second Street, NE
Washington, D.C. 20002



Anita Sheth
Director, Regulatory Policy Studies
Citizens for a Sound Economy
1250 H Street, NW
Suite 700
Washington, D.C. 20005

52/ Id. at 3502-03.